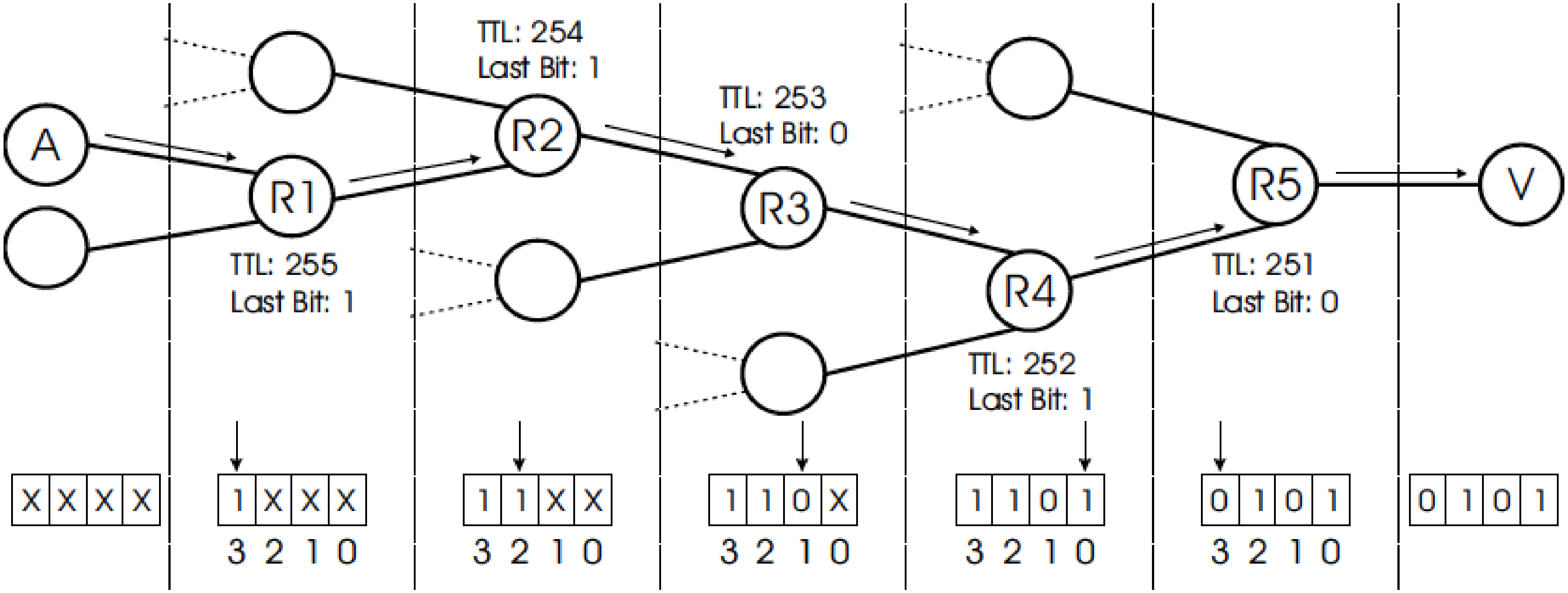
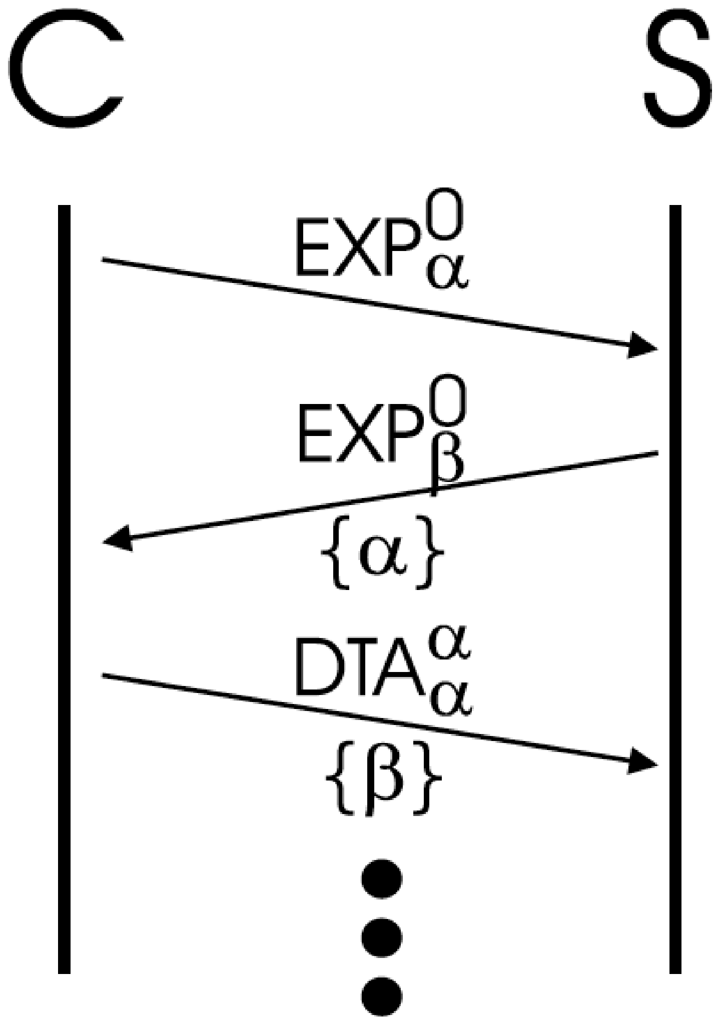


Figure 3. Example of our initial marking scheme. The packet travels from the attacker A to the victim V across the routers R1 to R5. Each router uses the TTL value of the packet to index into the IP identification field to insert its marking. In this example we show a 1-bit marking in a 4-bit field for simplicity.

The main shepherding consideration that's not already that explicit in the reviews is that the tone of the paper should emphasize the main contribution as being conceptual - the very nifty notion that one can tell in the core that the receiver consents to some on-going communication, and do this in a stateless fashion - rather than the practicality (which the PC found controversial).



Legend:

Pkt. Type$^{x}_{y}$ →
{Opt. Hdr.}

x - Sender initialized marking field

y - Marking Field at destination

C - Client

S - Server

	$x = 2$	$x = 3$	$x = 4$	$x = 5$
$z = 1$	0.7500	0.8750	0.9375	0.9688
$z = 2$	0.4375	0.5781	0.6836	0.7627
$z = 3$	0.2344	0.3301	0.4138	0.4871
$z = 4$	0.1211	0.1760	0.2275	0.2758

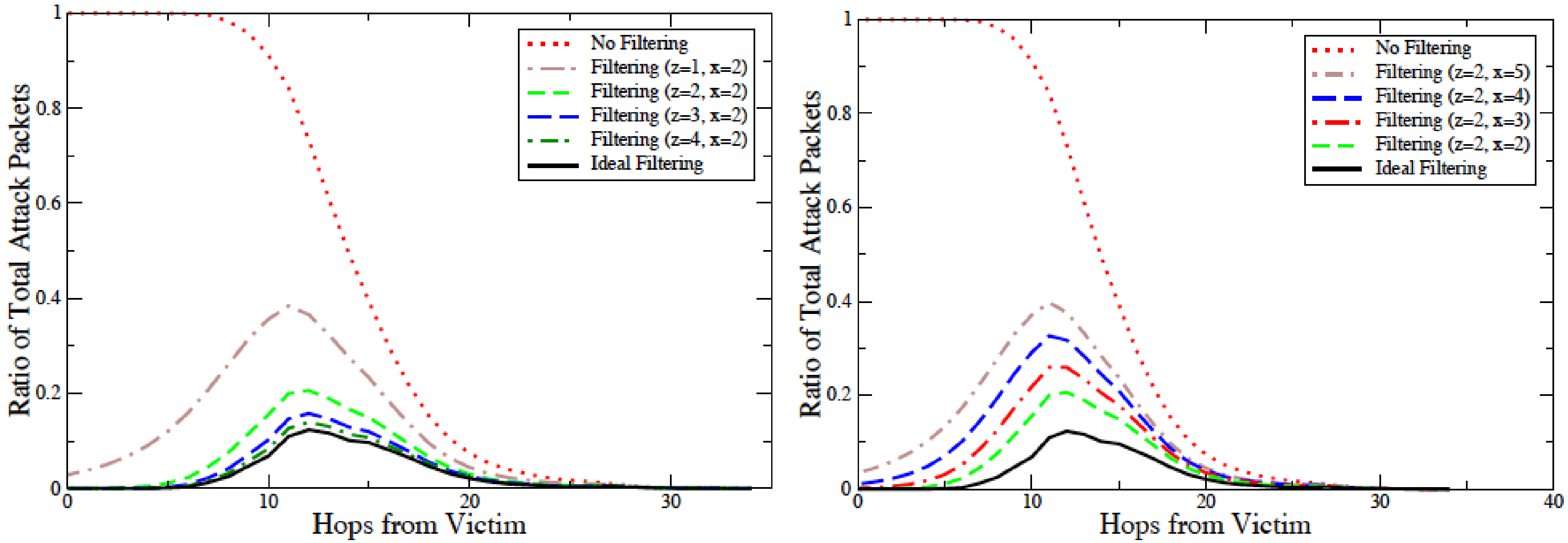
Table 1. Evaluation of $P(x, z)$ (the probability to pass one router with a forged probability), for common values of x and z.

The probability that the client can connect after k tries is:

$$\begin{aligned} &P(\text{ connect after k tries}) \\ &\quad = 1 - (1 - P(\text{connect after 1 try}))^k \\ &\quad = 1 - (1 - (1 - \epsilon_i)^i)^k \end{aligned}$$

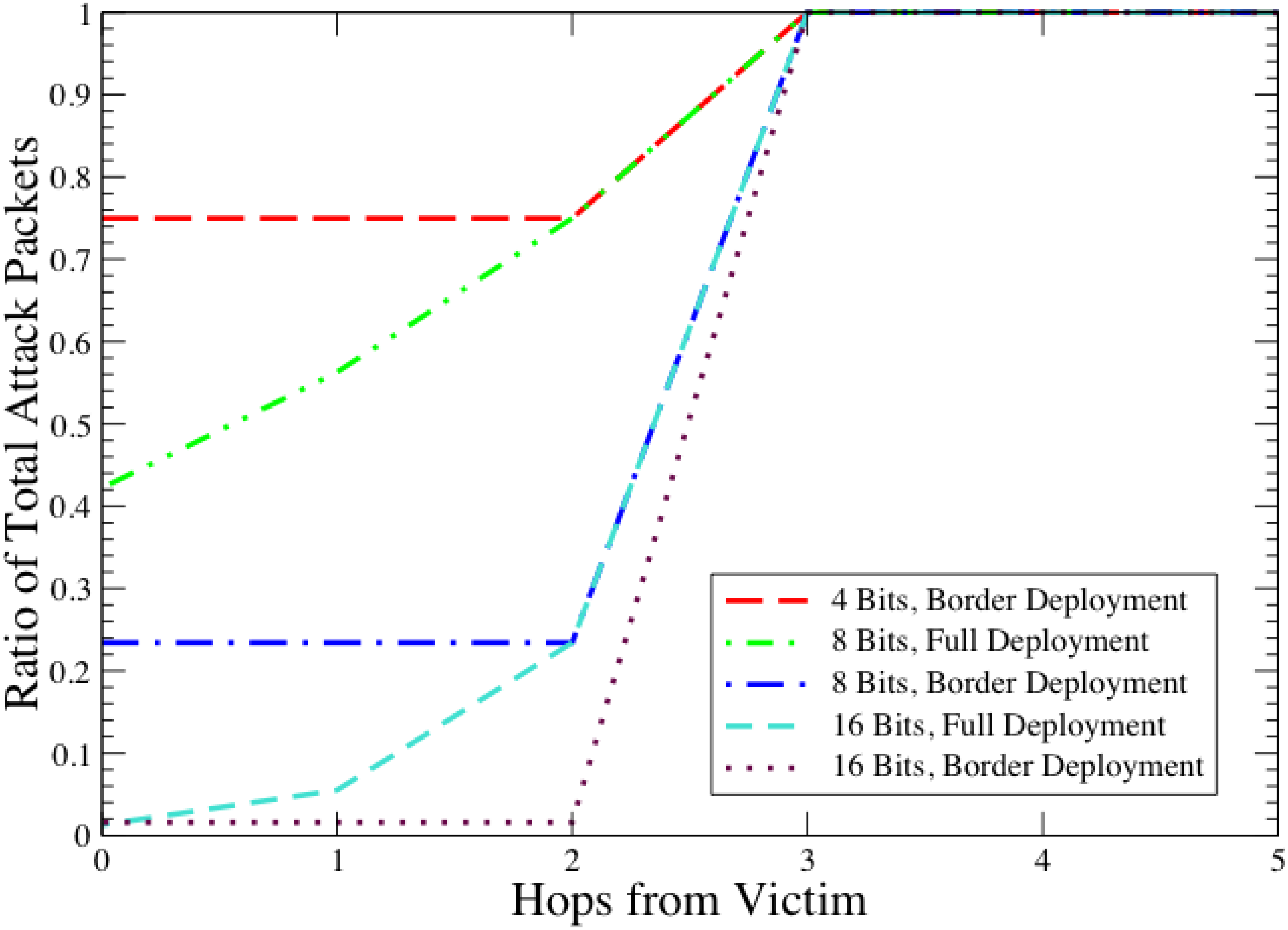
the required number of connection attempts is:

$$k = \frac{\log(1 - P(connect))}{\log(1 - (1 - \epsilon_i)^i)}$$



(a) Performance for various values of z, $(x = 2)$.

(b) Performance for various values of x, $(z = 3)$.



Ratio of Total Attack Packets
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
1
2
3
4
5
Hops from Victim
4 Bits, Border Deployment
8 Bits, Full Deployment
8 Bits, Border Deployment
16 Bits, Full Deployment
16 Bits, Border Deployment